PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-083233
(43)Date of publication of application : 21.03.2000

(51)Int.Cl. H04N 7/16
G06F 13/00
H04H 1/00
H04L 9/32
H04N 5/91
H04N 5/93
H04N 7/24
H04N 7/173

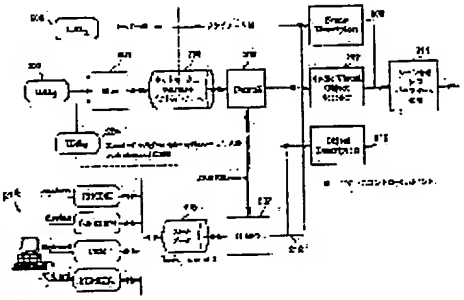
(21)Application number : 10-295936
(22)Date of filing : 16.10.1998

(71)Applicant : CANON INC
(72)Inventor : INOUE YUJI
NAKAGAWA TOSHIYUKI

(30)Priority
Priority number : 10183034 Priority date : 29.06.1998 Priority country : JP

(54) AUTHENTICATION DEVICE AND METHOD AND SYSTEM THEREFOR AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To attain the valid protection of copyrights and the valid use of a work by comparing authorization information included in received moving image data with inputted characters and symbols, and transmitting an instruction signal for instructing the re-reproduction of moving image data from reproduced initial image data to an outside information processor.
SOLUTION: A client divides a received MPEG-4 bit stream 205 into plural streams such as plural objects or the information of URL accompanying the objects by a demultiplexer 206. In this case, the information of the URL accompanying each object is transmitted to an IPMPS 207, and any URL information is selected, and an authentication request signal is transmitted to a multiplexer 201 having the corresponding URL connected on a network. When an access permission signal is received from the multiplexer 201, an access can be performed to an object whose access permission is obtained.



LEGAL STATUS
[Date of request for examination] 29.09.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－83233
（P2000－83233A）
(43)公開日　平成12年３月21日(2000.3.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｎ　7/16		Ｈ０４Ｎ	7/16	Ｚ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ	1/00	Ｚ
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ	7/173	６１０Ｚ
Ｈ０４Ｎ　5/91		Ｈ０４Ｌ	9/00	６７５Ａ

審査請求　未請求　請求項の数34　ＯＬ　（全 24 頁）　最終頁に続く

(21)出願番号　特願平10－295936

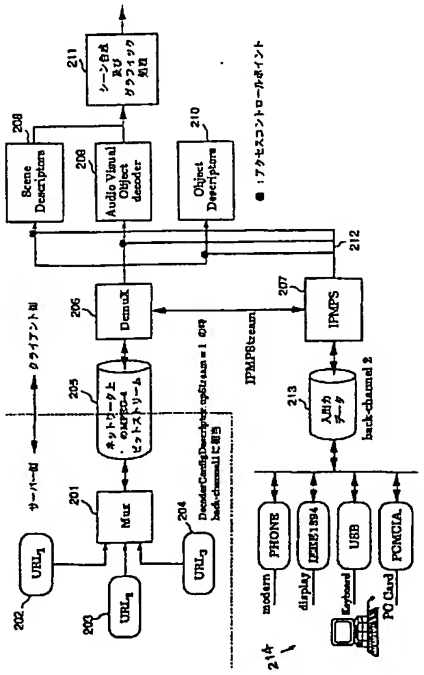
(22)出願日　平成10年10月16日(1998.10.16)

(31)優先権主張番号　特願平10－183034
(32)優先日　平成10年６月29日(1998.6.29)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　井上　裕司
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(72)発明者　中川　利之
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　（外２名）

(54)【発明の名称】　認証装置及び認証方法及び認証システム並びに記憶媒体

(57)【要約】
【課題】　オブジェクトの集合で構成される動画を再生するシステムにおいて、各オブジェクトの認証を効率的に行うとともに、認証処理に関わる遅延時間により再生映像が欠落する問題を解消する。
【解決手段】　オブジェクトの再送を要求する信号を、その要求先のサーバの出所情報と、認証結果を示す情報とともに、ｂａｃｋ－ｃｈａｎｎｅｌ　１（２０５）又は２（２１３）を使用して、認証を要求するオブジェクトの配信サーバ（２０２～２０４）へと送信する。



【特許請求の範囲】

【請求項１】　外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、
前記受信手段により受信された動画像データの一部を再生する再生手段と、
文字・記号を入力する入力手段と、前記受信手段により受信された動画像データに含まれる利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記外部情報処理装置へと送信する送信手段とを具備したことを特徴とする認証装置。

【請求項２】　前記動画像データは、圧縮符号化された動画像データであることを特徴とする請求項１に記載の認証装置。

【請求項３】　前記文字・記号をあらかじめ記憶した記憶手段を有し、前記比較手段は、前記受信手段により受信された動画像データに含まれる利用許可情報と、前記記憶手段に記憶された文字・記号とを比較することを特徴とする請求項１に記載の認証装置。

【請求項４】　前記再生手段は、前記動画像データの時間的一部分若しくは空間的一部分を再生することを特徴とする請求項１に記載の認証装置。

【請求項５】　前記送信手段は、前記指示信号と共に、当該認証装置が前記動画像データを利用可能であることを示す信号を送信することを特徴とする請求項１に記載の認証装置。

【請求項６】　前記送信手段は、通常、前記動画像データの受信用に使用されるインターフェースを、通常の方向に使用して前記動画像データを受信する他、通常の方向と逆方向に使用して前記指示信号を送信することを特徴とする請求項１に記載の認証装置。

【請求項７】　前記送信手段は、ＭＰＥＧ４のビットストリームのアップストリームを使用して、前記指示信号を送信することを特徴とする請求項１に記載の認証装置。

【請求項８】　通信回線と接続するインターフェースを更に具備し、前記送信手段は、前記インターフェース及び前記通信回線を介して、前記指示信号を送信することを特徴とする請求項１に記載の認証装置。

【請求項９】　出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、前記受信手段により受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離手段と、前記分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、前記分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備したことを特徴とする認証装置。

【請求項１０】　前記出所情報は、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）の情報であることを特徴とする請求項９に記載の認証装置。

【請求項１１】　外部情報処理方法より利用許可情報を含む動画像データを受信する受信ステップと、
前記受信ステップにより受信された動画像データの一部を再生する再生ステップと、
文字・記号を入力する入力ステップと、前記受信ステップにより受信された動画像データに含まれる利用許可情報と、前記入力ステップにより入力された文字・記号とを比較する比較ステップと、前記比較ステップによる比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生ステップにより再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする認証方法。

【請求項１２】　前記動画像データは、圧縮符号化された動画像データであることを特徴とする請求項１１に記載の認証方法。

【請求項１３】　前記文字・記号をあらかじめ記憶した記憶ステップを有し、前記比較ステップは、前記受信ステップにより受信された動画像データに含まれる利用許可情報と、前記記憶ステップに記憶された文字・記号とを比較することを特徴とする請求項１１に記載の認証方法。

【請求項１４】　前記再生ステップは、前記動画像データの時間的一部分若しくは空間的一部分を再生することを特徴とする請求項１１に記載の認証方法。

【請求項１５】　前記送信ステップは、前記指示信号と共に、当該認証方法が前記動画像データを利用可能であることを示す信号を送信することを特徴とする請求項１１に記載の認証方法。

【請求項１６】　前記送信ステップは、通常、前記動画像データの受信用に使用されるインターフェースを、通常の方向に使用して前記動画像データを受信する他、通常の方向と逆方向に使用して前記指示信号を送信することを特徴とする請求項１１に記載の認証方法。

【請求項１７】　前記送信ステップは、ＭＰＥＧ４のビ

ットストリームのアップストリームを使用して、前記指示信号を送信することを特徴とする請求項１１に記載の認証方法。

【請求項１８】　通信回線と接続するインターフェースを更に具備し、前記送信ステップは、前記インターフェース及び前記通信回線を介して、前記指示信号を送信することを特徴とする請求項１１に記載の認証方法。

【請求項１９】　出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信ステップと、
前記受信ステップにより受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離ステップと、
前記分離ステップにより分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生ステップと、
文字・記号を入力する入力ステップと、
前記分離ステップにより分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力ステップにより入力された文字・記号とを比較する比較ステップと、
前記比較ステップによる比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生ステップにより再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする認証方法。

【請求項２０】　前記出所情報は、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）の情報であることを特徴とする請求項１９に記載の認証方法。

【請求項２１】　互いに通信可能に接続された情報処理装置と認証装置とを有する認証システムであって、前記認証装置が、
前記情報処理装置から利用許可情報を含む動画像データを受信する受信手段と、
前記受信手段により受信された動画像データの一部を再生する再生手段と、
文字・記号を入力する入力手段と、
前記受信手段により受信された動画像データに含まれる利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記情報処理装置へと送信する送信手段とを具備したことを特徴とする認証システム。

【請求項２２】　少なくとも１つの情報処理装置と、該情報処理装置と互いに通信可能に接続された認証装置とを有する認証システムであって、前記認証装置が、
前記情報処理装置から出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、
前記受信手段により受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離手段と、
前記分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、
文字・記号を入力する入力手段と、
前記分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、
前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する前記情報処理装置へと送信する送信手段とを具備したことを特徴とする認証システム。

【請求項２３】　装置が実行可能なプログラムを格納する記憶媒体であって、前記プログラムを実行する装置を、
外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、
前記受信手段により受信された動画像データの一部を再生する再生手段と、
文字・記号を入力する入力手段と、
前記受信手段により受信された動画像データに含まれる利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、
前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする記憶媒体。

【請求項２４】　装置が実行可能なプログラムを格納する記憶媒体であって、前記プログラムを実行する装置を、
出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、
前記受信手段により受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離手段と、
前記分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、
前記分離手段により分離されたオブジェクトデータのう

ち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、
前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする記憶媒体。
【請求項２５】　出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、
前記分離手段により分離された複数の出所情報を管理する管理手段と、
前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、
前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、
前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段と、
を具備することを特徴とする認証装置。
【請求項２６】　前記出所情報は、ＵＲＬ（Uniform Resource Locator）の情報であることを特徴とする請求項２５に記載の認証装置。
【請求項２７】　前記複数のオブジェクトデータから構成される画像データは、圧縮符号化された動画データであることを特徴とする請求項２５に記載の認証装置。
【請求項２８】　前記管理手段により管理される任意の出所情報を選択する選択手段を更に具備することを特徴とする請求項２５に記載の認証装置。
【請求項２９】　前記送信手段は、通常、前記複数のオブジェクトデータから構成される画像データの受信用に使用されるインターフェースを、通常の方向に使用して前記画像データを受信する他、前記インターフェースを通常の方向と逆方向に使用して前記認証信号を送信することを特徴とする請求項２５に記載の認証装置。
【請求項３０】　前記送信手段は、ＭＰＥＧ４のビットストリームのアップストリームを使用して、前記認証信号を送信することを特徴とする請求項２５に記載の認証装置。
【請求項３１】　通信回線と接続するインターフェースを更に具備し、
前記送信手段は、前記インターフェース及び前記通信回線を介して、前記情報機器に対して前記認証信号を送信し、
前記受信手段は、前記通信回線及び前記インターフェースを介して、前記情報機器から前記許可信号を受信する、
ことを特徴とする請求項２５に記載の認証装置。
【請求項３２】　出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離工程と、
前記分離工程で分離された複数の出所情報を管理する管理工程と、
前記管理工程で管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信工程と、
前記送信工程で送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信工程と、
前記受信工程で受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御工程と、
を含むことをことを特徴とする認証方法。
【請求項３３】　各々ネットワークに接続して使用される情報機器と認証装置とを有する認証システムであって、前記認証装置が、
出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、
前記分離手段により分離された複数の出所情報を管理する管理手段と、
前記管理手段により管理される任意の出所情報により特定されるネットワーク上の前記情報機器に対して認証信号を送信する送信手段と、
前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、
前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段と、
を具備することを特徴とする認証システム。
【請求項３４】　認証処理を制御するプログラムを格納した記憶媒体であって、該プログラムを読み込んで実行する装置を、
出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、
前記分離手段により分離された複数の出所情報を管理する管理手段と、
前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、
前記送信手段により送信された認証信号に応答して前記

情報機器が送信した許可信号を受信する受信手段と、
前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段と、
を具備する装置として動作させることを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、認証装置及び認証方法及び認証システム並びに記憶媒体に係り、例えば、動画を再生する際に個々のオブジェクトに関して著作権保護等の目的で認証が必要となる場合に好適な認証装置及び認証方法及び認証システム並びに記憶媒体に関するものである。

【０００２】

【従来の技術】図１は、従来のデジタル映像データの送受信システムを示す図である。図１に示すように、デジタル映像データの配信サーバー１０は、それに付随したハードディスク等のデジタル映像データの記憶装置１２に予め記録されているデジタル映像データを、デジタル映像データの受信クライアント２０からの要求に応じてインターネット等のネットワーク網３０を介して受信クライアント２０にダウンロードする。ここで、配信サーバー１０は、デジタル映像データを符号化する変換部１１を有し、この変換部１１によりデジタル映像データを符号化してデータ量を削減し、これをＴＣＰ／ＩＰプロトコル等の手順に従って受信クライアント２０に配信する。受信クライアント２０側は、デジタル映像データを復号する変換部２１を有し、この変換部２１により受信に係るデジタル映像信号を再生し、表示、記録又は編集に供する。

【０００３】１つの動画シーンを複数のオブジェクトで構成し、配信サーバー１０の変換部１１において各々のオブジェクトを符号化して圧縮し、これを受信クライアント２０に転送し、受信クライアント２０において、これらを復号し、再構成して動画シーンを再生するシステムの一例としてＭＰＥＧ－４プレーヤーがある。

【０００４】図２は、従来のＭＰＥＧ－４プレーヤーの構成図である。図２は、「ＩＳＯ／ＩＥＣ　ＦＣＤ　１４４９６－１　Ｆｉｇ．１－１」に基づいて記載されたものであり、その詳しい説明については、「ＩＳＯ／ＩＥＣ　ＦＣＤ　１４４９６－１」において述べられている。ここでは、その概略についてのみ説明する。

【０００５】ネットワーク等を介して転送（ｔｒａｎｓｍｉｓｓｉｏｎ）されたＭＰＥＧ－４　ビットストリームやＤＶＤ－ＲＡＭ等の記録メディア（ｓｔｒａｇｅ　ｍｅｄｉｕｍ）から読み出されたＭＰＥＧ－４　ビットストリームは、「ＴｒａｎｓＭｕｘ　Ｌａｙｅｒ」において、転送／読み出しに相当する手順に従って受け取られ（ｓｅｓｓｉｏｎの確立）、「ＦｌｅｘＭｕｘ」部において、シーン記述データ、オブジェクトデータ、オブジェクト記述データの各ストリームに分離し、復号し、再生され、シーン記述データ（ｓｃｅｎｅ　ｄｅｓｃｒｉｐｔｉｏｎｉｎｆｏｒｍａｔｉｏｎ）に基づいて、シーンが再生或いはグラフィック処理される。

【０００６】なお、図３は、図２を模式化、簡略化したものである。ここで、個々のオブジェクトについて著作権保護等の目的で認証が必要となる場合、シーン記述データを含む複数のオブジェクトデータを含むビットストリームに「ＩＰ　ＤａｔａＳｅｔ」（著作権情報群）を含ませることが考えられる。

【０００７】

【発明が解決しようとする課題】しかしながら、転送ビットストリームに「ＩＰ　Ｄａｔａ　Ｓｅｔ」（著作権情報群）を含ませた場合でも、図２若しくは図３に示す構成では、仮に「Ｏｂｊｅｃｔ　Ｄｅｓｃｒｉｐｔｏｒｓ」において「ＩＰ　Ｄａｔａ」が再生されたとしても、画像の再生処理の際に「ＩＰ　Ｄａｔａ」についての処理がなされないため、「ＩＰ　Ｐｒｏｔｅｃｔｉｏｎ」（著作権保護）処理が実行されることがない。

【０００８】もちろん、この場合でもデコードされた「ＩＰ　Ｄａｔａ　Ｓｅｔ」をアプリケーションが受け取って「ＩＰ　Ｐｒｏｔｅｃｔｉｏｎ」処理を実行することは可能であるが、この場合の処理はそのアプリケーションに固有の処理であり、他のプレーヤーや他の機種において同様の処理が実行されるとは限らない。

【０００９】また、図２若しくは図３に示す構成では、個々のオブジェクトに対して認証処理を行った後に画像を再生するため、動画シーンを再生する際に次々と新しいオブジェクトが出現する場合には、その度に再生を一時的に停止して認証を求める必要があった。さらに、認証処理を行う際に、再生を停止しないでおくと、当然のことながら、認証処理にかかった時間分だけ、再生される映像が欠落してしまうという問題があった。

【００１０】本発明は、上記の背景に鑑みてなされたものであり、例えば、認証処理を効率化し、著作権等の有効な保護と著作物の有効な利用を図るとともに、認証処理に関わる遅延時間により再生映像が欠落する問題を解消することを目的とする。

【００１１】

【課題を解決するための手段】本発明の第１の側面に係る認証装置は、外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、受信手段により受信された動画像データに含まれる利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するよう

に指示する指示信号を、外部情報処理装置へと送信する送信手段とを具備したことを特徴とする。

【００１２】上記の認証装置において、動画像データは、例えば、圧縮符号化された動画像データであることが好ましい。

【００１３】上記の認証装置において、例えば、文字・記号をあらかじめ記憶した記憶手段を更に有し、比較手段は、例えば、受信手段により受信された動画像データに含まれる利用許可情報と、記憶手段に記憶された文字・記号とを比較することが好ましい。

【００１４】上記の認証装置において、再生手段は、例えば、動画像データの時間的一部分若しくは空間的一部分を再生することが好ましい。

【００１５】上記の認証装置において、送信手段は、例えば、指示信号と共に、当該認証装置が動画像データを利用可能であることを示す信号を送信することが好ましい。

【００１６】上記の認証装置において、送信手段は、例えば、通常、動画像データの受信用に使用されるインターフェースを、通常の方向に使用して動画像データを受信する他、通常の方向と逆方向に使用して指示信号を送信することが好ましい。

【００１７】上記の認証装置において、送信手段は、例えば、ＭＰＥＧ４のビットストリームのアップストリームを使用して、指示信号を送信することが好ましい。

【００１８】上記の認証装置において、例えば、通信回線と接続するインターフェースを更に具備し、送信手段は、例えば、インターフェース及び通信回線を介して、指示信号を送信することが好ましい。

【００１９】本発明の第２の側面に係る認証装置は、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、受信手段により受信された動画像データを複数のオブジェクトデータの各々に分離する分離手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備したことを特徴とする。

【００２０】上記の認証装置において、出所情報は、例えば、ＵＲＬ（ＵｎｉｆｏｒｍＲｅｓｏｕｒｃｅＬｏｃａｔｏｒ）の情報であることが好ましい。

【００２１】本発明の第３の側面に係る認証方法は、外部情報処理方法より利用許可情報を含む動画像データを受信する受信ステップと、受信ステップにより受信された動画像データの一部を再生する再生ステップと、文字・記号を入力する入力ステップと、受信ステップにより受信された動画像データに含まれる利用許可情報と、入力ステップにより入力された文字・記号とを比較する比較ステップと、比較ステップによる比較の結果、利用許可情報と文字・記号とが一致した場合に、再生ステップにより再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする。

【００２２】上記の認証方法において、動画像データは、例えば、圧縮符号化された動画像データであることが好ましい。

【００２３】上記の認証方法において、例えば、文字・記号をあらかじめ記憶した記憶ステップを更に有し、比較ステップは、例えば、受信ステップにより受信された動画像データに含まれる利用許可情報と、記憶ステップに記憶された文字・記号とを比較することが好ましい。

【００２４】上記の認証方法において、再生ステップは、例えば、動画像データの時間的一部分若しくは空間的一部分を再生することが好ましい。

【００２５】上記の認証方法において、送信ステップは、例えば、指示信号と共に、当該認証方法が動画像データを利用可能であることを示す信号を送信することが好ましい。

【００２６】上記の認証方法において、送信ステップは、例えば、通常、動画像データの受信用に使用されるインターフェースを、通常の方向に使用して動画像データを受信する他、通常の方向と逆方向に使用して指示信号を送信することが好ましい。上記の認証方法において、送信ステップは、例えば、ＭＰＥＧ４のビットストリームのアップストリームを使用して、指示信号を送信することが好ましい。

【００２７】上記の認証方法において、例えば、通信回線と接続するインターフェースを更に具備し、送信ステップは、例えば、インターフェース及び通信回線を介して、指示信号を送信することが好ましい。

【００２８】本発明の第４の側面に係る認証方法は、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信ステップと、受信ステップにより受信された動画像データを複数のオブジェクトデータの各々に分離する分離ステップと、分離ステップにより分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生ステップと、文字・記号を入力する入力ステップと、分離ステップにより分離されたオブジェクトデータのうち、利用許可情報を

含むオブジェクトデータに関して、当該利用許可情報と、入力ステップにより入力された文字・記号とを比較する比較ステップと、比較ステップによる比較の結果、利用許可情報と文字・記号とが一致した場合に、再生ステップにより再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする。上記の認証方法において、出所情報は、例えば、ＵＲＬ（ＵｎｉｆｏｒｍＲｅｓｏｕｒｃｅＬｏｃａｔｏｒ）の情報であることが好ましい。

【００２９】本発明の第５の側面に係る認証システムは、互いに通信可能に接続された情報処理装置と認証装置とを有する認証システムであって、認証装置が、情報処理装置から利用許可情報を含む動画像データを受信する受信手段と、受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、受信手段により受信された動画像データに含まれる利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、情報処理装置へと送信する送信手段とを具備したことを特徴とする。本発明の第６の側面に係る認証システムは、少なくとも１つの情報処理装置と、該情報処理装置と互いに通信可能に接続された認証装置とを有する認証システムであって、認証装置が、情報処理装置から出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、受信手段により受信された動画像データを複数のオブジェクトデータの各々に分離する分離手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する情報処理装置へと送信する送信手段とを具備したことを特徴とする。

【００３０】本発明の第７の側面に係る記憶媒体は、装置が実行可能なプログラムを格納する記憶媒体であって、プログラムを実行する装置を、外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、受信手段により受信された動画像データに含まれる利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする。

【００３１】本発明の第８の側面に係る記憶媒体は、装置が実行可能なプログラムを格納する記憶媒体であって、プログラムを実行する装置を、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、受信手段により受信された動画像データを複数のオブジェクトデータの各々に分離する分離手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする。

【００３２】本発明の第９の側面に係る認証装置は、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段とを具備することを特徴とする。

【００３３】上記の認証装置において、前記出所情報は、例えばＵＲＬ（Uniform ResourceLocator）の情報であることが好ましい。

【００３４】上記の認証装置において、前記複数のオブジェクトデータから構成される画像データは、例えば、圧縮符号化された動画データであることが好ましい。

【００３５】上記の認証装置において、例えば、前記管

理手段により管理される任意の出所情報を選択する選択手段を更に具備することが好ましい。

【００３６】上記の認証装置において、例えば、前記送信手段は、通常、前記複数のオブジェクトデータから構成される画像データの受信用に使用されるインターフェースを、通常の方向に使用して前記画像データを受信する他、前記インターフェースを通常の方向と逆方向に使用して前記認証信号を送信することが好ましい。

【００３７】上記の認証装置において、前記送信手段は、例えば、ＭＰＥＧ４のビットストリームのアップストリームを使用して、前記認証信号を送信することが好ましい。

【００３８】上記の認証装置において、通信回線と接続するインターフェースを更に具備し、前記送信手段は、前記インターフェース及び前記通信回線を介して、前記情報機器に対して前記認証信号を送信し、前記受信手段は、前記通信回線及び前記インターフェースを介して、前記情報機器から前記許可信号を受信することが好ましい。

【００３９】本発明の第１０の側面に係る認証方法は、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離工程と、前記分離工程で分離された複数の出所情報を管理する管理工程と、前記管理工程で管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信工程と、前記送信工程で送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信工程と、前記受信工程で受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御工程とを含むことをことを特徴とする。

【００４０】本発明の第１１の側面に係る認証システムは、各々ネットワークに接続して使用される情報機器と認証装置とを有する認証システムであって、前記認証装置が、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の前記情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段とを具備することを特徴とする。

【００４１】本発明の第１２の側面に係る記憶媒体は、認証処理を制御するプログラムを格納した記憶媒体であって、該プログラムを読み込んで実行する装置を、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段とを具備する装置として動作させることを特徴とする。

【００４２】

【発明の実施の形態】以下、添付図面を参照しながら本発明の好適な実施の形態を説明する。以下の実施の形態は、所謂「ｂａｃｋ－ｃｈａｎｎｅｌ」を利用して認証処理を効率化したシステムに関する。

【００４３】（第１の実施形態）図４は、本発明の好適な実施の形態に係るＭＰＥＧ－４プレーヤーを含むシステムの概略構成を示す図である。図４に示すシステムは、「ＩＰ　Ｄａｔａ　Ｓｅｔ」を操作して「ＩＰ　Ｐｒｏｔｅｃｔｉｏｎ」を実現するシステムである。図４に示すシステムは、ＩＰＭＰＳ　（Ｉｎｔｅｌｌｅｃｔｕａｌ　Ｐｒｏｐｅｒｔｙ　Ｍａｎａｇｅｍｅｎｔ　ａｎｄ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）２０７を有し、このＩＰＭＰＳ２０７により著作権認証及び保護機能を実現する点で図３に示すシステムと異なる。

【００４４】図７は、認証処理に関するクライアントの動作を示すフローチャートである。以下、図７を参照しながら図４に示すシステムの動作を説明する。サーバー側では、マルチプレクサ２０１が、各々異なるＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）としてＵＲＬ１、ＵＲＬ２、ＵＲＬ３を持つ複数のネットワーク・サイト２０２～２０４から、夫々個々のオブジェクトを受信してこれらの複数のオブジェクトで構成される動画データを生成する。この動画データは、クライアントからの要求に応じてＭＰＥＧ－４ビットストリーム２０５としてネットワークを介してクライアントに送信される。

【００４５】ステップＳ１では、クライアントは、サーバーよりＭＰＥＧ－４ビットストリーム２０５を受信する。このＭＰＥＧ－４ビットストリームを構成する各オブジェクトには、著作権の帰属先を示す情報（ここでは、ＵＲＬの情報）が付随している。ステップＳ２では、クライアントは、受信に係るＭＰＥＧ－４ビットストリームをデマルチプレクサ２０６により複数のオブジェクトやそれに付随する情報（ＵＲＬの情報を含む）等の複数のストリームに分離する。ここで、各オブジェク

トに付随するＵＲＬの情報は、「ＩＰ　Ｄａｔａ」のストリームである「ＩＰＭＰＳ　Ｓｔｒｅａｍ」の一部としてＩＰＭＰＳ２０７に送られる。

【００４６】ステップＳ３では、ＩＰＭＰＳ２０７に送られた１又は複数のＵＲＬの情報の中から、いずれか１つのＵＲＬの情報を選択する。これは、例えば、操作者が指定するものであっても構わないし、所定の順序に従ってＩＰＭＰＳ２０７が選択しても構わない。

【００４７】ステップＳ４では、選択したＵＲＬの情報に基づいて、ネットワーク上に接続された１又は複数のサーバのうち対応するＵＲＬを持つサーバ２０１に対して認証依頼信号を送信する。この場合、その送信には、後述するバックチャネル（ｂａｃｋ－ｃｈａｎｎｅｌ）１又はバックチャネル（ｂａｃｋ－ｃｈａｎｎｅｌ）２が使用される。

【００４８】ステップＳ５では、認証依頼信号を受け取ったサーバ２０１からアクセス許可信号が送信されてくるのを待ち、アクセス許可信号を受信した場合はステップＳ６に進み、所定時間内にアクセス許可信号を受信しなかった場合はステップＳ７に進む。

【００４９】ステップＳ６では、アクセス許可信号の受信によりアクセス許可（認証）が得られたオブジェクトに対するアクセスを可能にする。具体的には、アクセスコントロールポイントを制御する制御信号２１２を許可状態にすることにより、シーン・ディスクリプタ２０８、オーディオ・ビジュアル・デコーダ２０９、オブジェクトディスクリプタ２１０がデマルチプレクサ２０６の該当するストリーム（即ち、アクセス許可信号によりアクセスを許可されたオブジェクトのストリーム）にアクセスすることを可能にする。

【００５０】一方、ステップＳ７では、アクセスコントロールポイントを制御する制御信号２１２を禁止状態にすることにより、シーン・ディスクリプタ２０８、オーディオ・ビジュアル・デコーダ２０９、オブジェクトディスクリプタ２１０がデマルチプレクサ２０６の該当するストリーム（即ち、認証を依頼したがアクセス許可が得られなかったオブジェクトのストリーム）にアクセスすることを禁止する。

【００５１】ステップＳ８では、他のオブジェクトに付随するＵＲＬの情報があるか否かを確認し、当該ＵＲＬの情報があればステップＳ３に戻り、なければ一連の処理を終了する。

【００５２】シーン合成・グラフィック処理部２１１は、シーン・ディスクリプタ２０８、オーディオ・ビジュアル・デコーダ２０９、オブジェクトディスクリプタ２１０から供給されるデータに基づいて、シーン合成及びグラフィック処理を行う。この際、アクセス許可が得られたオブジェクトのみを再生の際の合成の対象としても良いし、１つでもアクセス許可が得られなかったオブジェクトがある場合に、一切の再生を行わないようにしても良い。

【００５３】以下、上述した認証処理について更に詳細に説明する。

【００５４】ＭＰＥＧ－４ビットストリームは、オブジェクト単位のビットストリームである「Ｅｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ」（ＥＳ）の内容を記述する「ＥＳ＿Ｄｅｓｃｒｉｐｔｏｒ」と、オブジェクト自身を記述する「ＯＤ＿Ｄｅｓｃｒｉｐｔｏｒ」を含む。ここで、「ＥＳ＿Ｄｅｓｃｒｉｐｔｏｒ」或いは「ＯＤ＿Ｄｅｓｃｒｉｐｔｏｒ」に、リモートアクセスのためのコマンドとアクセス先を指定するＵＲＬの情報が含まれている場合は、図５に示すような手順でリモートアクセスが実行される。

【００５５】図５は、リモートアクセスを説明する簡略図である。図５において、「ＤＡＩ」は、「ＤＭＩＦ　Ａｐｐｌｉｃａｔｉｏｎ　Ｉｎｔｅｒｆａｃｅ」と呼ばれる、ＭＰＥＧ－４ビットストリームとネットワークとのインターフェース層である。この詳細については、「ＩＳＯ／ＩＥＣ　１４４９６－６　ＤＭＩＦドキュメントＤＭＩＦ　Ａｐｐｌｉｃａｔｉｏｎ　Ｉｎｔｅｒｆａｃｅ」の項に記載されているため、ここでは省略する。

【００５６】また、ＭＰＥＧ－４ビットストリームは、「ｅｌｅｍｅｎｔａｒｙ　ｓｔｒｅａｍ」（ＥＳ）に対応したデコーダの種類についての情報を示す「ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ」を含む。この「ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ」は、幾つかのデータ要素の構造体であり、その中の要素の一つにストリーム型を示す１ビットのｕｐＳｔｒｅａｍパラメータがある。この詳細については、「ＩＳＯ／ＩＥＣ　１４４９６－１　ＦＣＤ　８．３．４　ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ」の項に記載されているため、ここでは省略する。

【００５７】式１に、「ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ」の一例を挙げる。

【００５８】

[式１：DecoderConfigDescriptor]

```
aligned(8) class DecoderConfigDescriptor
              : bit(8) tag=DecoderConfigDescrTag {
      bit(8) length;
      bit(8) objectProfileIndication;
      bit(6) streamType;
      bit(1) upStream;
      const bit(1) reserved=1;
      bit(24) bufferSizeDB;
      bit(32) maxBitrate;
      bit(32) avgBitrate;
      DecoderSpecificInfo decSpecificInfo[];
}
```

【００５９】ここで、ストリームの識別は、式１の「Ｄ

ｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ」のクラス宣言中のデータ要素である「ｓｔｒｅａｍＴｙｐｅ」の値に基づいて行う。「ｓｔｒｅａｍＴｙｐｅ」の値は、表１のように定義されている。

【００６０】

【表１】

表1：ストリーム型指定値

ストリーム型指定値	ストリーム型
0x00	reserved for ISO use
0x01	ObjectDescriptorStream
0x02	ClockReferenceStream
0x03	SceneDescriptionStream
0x04	VisualStream
0x05	AudioStream
0x06	MPEG7Stream
0x07-0x09	reserved for ISO use
0x0A	ObjectContentInfoStream
0x0B	*IPMPStream*
0x0C - 0x1F	reserved for ISO use
0x20 - 0x3F	user private

【００６１】なお、表１は、「ＩＳＯ／ＩＥＣ　１４４９６－１　ＦＣＤ　Ｔａｂｌｅ　０－１：　ｓｔｒｅａｍＴｙｐｅ　Ｖａｌｕｅｓ」に対して、この実施の形態に固有の「ＩＰＭＰＳｔｒｅａｍ」を識別するための値を追加したものである。表１において、各パラメータや用語は、「ＩＳＯ／ＩＥＣ　１４４９６－１　ＦＣＤ」と同じであるので、ここでは説明を省略する。

【００６２】図４に示すように、ストリームの向きを示すフラグである「ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ．ｕｐＳｔｒｅａｍ」が”１”の時は、システムは、クライアント側からサーバ側にストリームを転送する「ｕｐｓｔｒｅａｍ」の状態になる。ここでは、この「ｕｐｓｔｒｅａｍ」の状態を利用した転送機能を「ｂａｃｋ－ｃｈａｎｎｅｌ１」と呼ぶことにする。

【００６３】通常の再生時は、「ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ．ｕｐＳｔｒｅａｍ」が”０”であり、サーバ側からクライアント側にストリームを転送する「ｄｏｗｎｓｔｒｅａｍ」の状態である。一方、オブジェクトに対するアクセスの許可を求める場合は、「ＤｅｃｏｄｅｒＣｏｎｆｉｇＤｅｓｃｒｉｐｔｏｒ．ｕｐＳｔｒｅａｍ」を”１”として、必要なデータをＵＲＬ先へ「ｕｐｓｔｒｅａｍ」する所謂「ｂａｃｋ－ｃｈａｎｎｅｌ１」を用いることにより、「ＩＰＭＰ　Ｍａｎａｇｅｍｅｎｔ　Ｄａｔａ」（著作権管理情報）を「ＩＰＭＰＳｔｒｅａｍ」としてサーバ側に送り、リモートアクセスによりＵＲＬ先から応答データを転送させることになる。

【００６４】表１に示す「ＩＰＭＰＳｔｒｅａｍ」は、「ＩＰＭＰ＿ＥＳ」と「ＩＰＭＰ＿Ｄ」の構成を有する。「ＩＰＭＰＳ＿ＥＳ」の各々は一連の「ＩＰＭＰ＿Ｍｅｓｓａｇｅｓ」からなる。　式２は「ＩＰＭＰ＿Ｍｅｓｓａｇｅｓ」の記述例である。

【００６５】

[式2:IPMP_Message]

```
class IPMP_Message () {
        unsigned int(8)      IPMPS_TypeCount;
        bit(1)  hasURL;
        int i;
        for (i = 0; i <; IPMPS_TypeCount; i++) {
                unsigned int(16) IPMPS_Type[[i]];
                unsigned int(32) offset[[i]];
                unsigned int(16) length[[i]];
        }
        if (hasURL) {
                unsigned int(5) lengthOfURLbits;
                bit(3) reserved=0b111;
                unsigned int(lengthOfURLbits) lengthOfURL;
                char(8) URLString[lengthOfURL];
```

```
        }
        for (i = 0; i <; IPMPS_TypeCount; i++) {
            char(8) IPMP_data[length[i]];
        }
    }
```

【００６６】式２において、「ＩＰＭＰＳ＿ＴｙｐｅＣｏｕｎｔ」は、異なる「ＩＰＭＰＳｔｙｐｅ」の数を表わす。これにより、異なるＩＰＭＰＳを存在させることが可能となるため、「ＩＰＭＰ ｍｅｓｓａｇｅｓ」は複数のＩＰＭＰＳに対応可能である。

【００６７】なお、ＵＲＬが指定されている場合は、「ＩＰＭＰＳ＿ＴｙｐｅＣｏｕｎｔ」は０を取り、その他は最低値である１を取る。また、この場合、内部の「ＩＰＭＰ＿Ｍｅｓｓａｇｅ」の代わりに、外部に格納されている「ＩＰＭＰ＿Ｍｅｓｓａｇｅ」を参照して使用することになる。

【００６８】また、「ＩＰＭＰＳ＿Ｄ」は、「ＩＰＭＰ Ｄｅｓｃｒｉｐｔｏｒ」からなる。この「ＩＰＭＰ Ｄｅｓｃｒｉｐｔｏｒ」は、個々の「ｅｌｅｍｅｎｔａｒｙ ｓｔｒｅａｍｓ」に対する詳細なＩＰＭＰ制御を行うためのデータ構造体である。そして、「ＩＰＭＰ Ｄｅｓｃｒｉｐｔｏｒ Ｕｐｄａｔｅｓ」は、オブジェクト・ディスクリプタ・ストリーム（Ｏｂｊｅｃｔ Ｄｅｓｃｒｉｐｔｏｒ ｓｔｒｅａｍ）の一部として実行される。式３は、「ＩＰＭＰ Ｄｅｓｃｒｉｐｔｏｒ Ｕｐｄａｔｅｓ」の記述例を示す。

【００６９】

[式3:IPMP_DescriptorUpdate]

```
aligned(8) class IPMP_DescriptorUpdate : uint(8) IPMP_DescriptorUpdateTa
g {
        unsigned int(8)      descriptorCount;
        int i;
        for (i = 0; i <; descriptorCount; i++) {
            IPMP_Descriptor      d[[i]];
        }
    }
```

【００７０】式３において、「ｄｅｓｃｒｉｐｔｏｒＣｏｕｎｔ」は、更新される「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒｓ」の数を表わし、また、ｄ［ｉ］は、あるーつの「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒ」を表わす。式４は、「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒ」の記述例を示す。

【００７１】

[式4:IPMP_Descriptor]

```
class IPMP_Descriptor () {
        bit(8)  IPMP_Descriptor_ID;
        unsigned int(8)      IPMPS_TypeCount;
        bit(1)  hasURL;
        int i;
        for (i = 0; i <; IPMPS_TypeCount; i++) {
            unsigned int(16)      IPMPS_Type[[i]];
            unsigned int(32) offset[[i]];
            unsigned int(16) length[[i]];
        }
        if (hasURL) {
            unsigned int(5) lengthOfURLbits;
            bit(3) reserved=0b111;
            unsigned int(lengthOfURLbits) lengthOfURL;
            char(8)   URLString[lengthOfURL];
        }
        for (i = 0; i <; IPMPS_TypeCount; i++) {
            char(8) IPMP_data[length[i]];
        }
    }
```

【００７２】式４において、「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒ＿ＩＤ」は、各「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒ」に固有の番号であり、「ＥＳ＿Ｄｅｓｃｒｉｐｔｏｒｓ」は、「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒ＿ＩＤ」を使って「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒｓ」を参照する。　また、「ＩＰＭＰＳ＿ＴｙｐｅＣｏｕｎｔ」は、「ＩＰＭＰ＿Ｍｅｓｓａｇｅ」で指定された異なるＩＰＭＰＳの数を表わす。

【００７３】図６は、ＵＲＬ先で更にＵＲＬ指定がある場合の階層構造の例を示す図である。なお、図６は２階層の場合の例であるが、もちろん、更なるＵＲＬ指定がある場合、３階層になっても４階層になってもよい。また、図６においては、「ＩＰＭＰＳｔｒｅａｍ」を明示していないが、リモート指定されるオブジェクト（Ｏｂｊｅｃｔ）に関する「ＩＰＭＰ＿ＥＳ」か「ＩＰＭＰ＿Ｄ」が、「ＳｃｅｎｅＤｅｓｃｒｉｐｔｉｏｎＳｔｒｅａｍ」か「ＯｂｊｅｃｔＤｅｓｃｒｉｐｔｉｏｎＳｔｒｅａｍ」に呼応して、必要に応じデコードされ、リモートアクセスされることは、先に説明した図５の場合と同様である。

【００７４】以上、ＭＰＥＧ－４のビットストリームの「ｕｐｓｔｒｅａｍ」の状態、即ち、バックチャネル（ｂａｃｋ－ｃｈａｎｎｅｌ）１を使用した認証処理について説明したが、このような「ｂａｃｋ－ｃｈａｎｎｅｌ１」を使用する認証処理は、リアルタイムのビットストリーム再生時における「ｕｐＳｔｒｅａｍ」処理であるので、比較的データ量が少なく処理時間の短い高速処理向けの場合を想定している。ここで、リアルタイム再生をしているシステムでは、「ｂａｃｋ－ｃｈａｎｎｅｌ１」によるリモートアクセス及び認証による遅延は極力少ないことが望ましい。

【００７５】しかしながら、データ量が少ない場合であっても認証に相応の時間を要することがあり、その場合、「ｂａｃｋ－ｃｈａｎｎｅｌ１」における遅延が問題となる。この場合、許容遅延時間の点、また、インタラクティブな操作性を必要とする点から考えると、第２の「ｂａｃｋ－ｃｈａｎｎｅｌ」を設けることが好ましい。

【００７６】そこで、この実施の形態では、ＭＰＥＧ－４のビットストリームを伝送するのとは異なるＩ／Ｏ（機器間入出力）インターフェースが設けられている。これを以下では「ｂａｃｋ－ｃｈａｎｎｅｌ２」と呼ぶことにする。

【００７７】まず、「ｂａｃｋ－ｃｈａｎｎｅｌ２」を使用した認証処理を説明する前に、「ｂａｃｋ－ｃｈａｎｎｅｌ１」と「ｂａｃｋ－ｃｈａｎｎｅｌ２」におけるデータ量と遅延時間の関係を考える。「ＭＰＥＧ－４　ＲｅｑｕｉｒｅｍｅｎｔＧｒｏｕｐ」の報告では、リアルタイム再生を妨げない「ｂａｃｋ－ｃｈａｎｎｅｌ」の遅延許容時間は１フレーム時間とあるので、これに基づいて「ｂａｃｋ－ｃｈａｎｎｅｌ１」と「ｂａｃｋ－ｃｈａｎｎｅｌ２」における想定データ量と転送レートの関係を求めると、表２のようになる。

【００７８】

【表２】

表記	使用目的	データ量	遅延時間
back-channel 1	認証のための高速 IPMP リモートアクセス	3000 - 5000 bits/s	100-300 ms
back-channel 2	認証のための低速 IPMP 入出力アクセス		>500ms

表２　back-channel １及び２の遅延時間とデータ量

【００７９】ここで、認証のための高速ＩＰＭＰリモートアクセスでは、１００－５００ｂｉｔ／Ｆｒａｍｅ以内のデータ量を３Ｋ－５Ｋ／ｓｅｃの転送ラインで処理することが遅延時間の限界となる。「ＩＰＭＰ＿Ｍｅｓｓａｇｅ」データや「ＩＰＭＰ＿Ｄｅｓｃｒｉｐｔｏｒ」データとＵＲＬ指定による「ｂａｃｋ－ｃｈａｎｎｅｌ」による「ｒｅｍｏｔｅ　ｃｏｎｔｅｎｔ　ａｃｃｅｓｓ」の結果としてのｄｅｌａｙ－ｂａｎｄｗｉｄｔｈの関係を、表４と見ることができるので、実際の認証のためのデータ量は限られたものになる。一方、認証には、ｓｔｒｅａｍ処理とは非同期に時間を要することが多い。

【００８０】また、複数のオブジェクトの認証が一箇所のサイトではなく、複数に跨ることも想定される。この場合には、表２の条件は更に厳しくなり、実用に耐えなくなる。そのため、ｓｔｒｅａｍ処理と非同期で低速処理が可能な認証手続きの場合には、「ｂａｃｋ－ｃｈａｎｎｅｌ　２」を用いた方が良い。

【００８１】以下、「ｂａｃｋ－ｃｈａｎｎｅｌ　２」を使用した場合の処理について説明する。認証のための低速ＩＰＭＰ入出力アクセスのための「ｂａｃｋ－ｃｈａｎｎｅｌ２」は、図４に示すように、基本的にはＭＰＥＧ－４ビットストリームを伝送するものとは異なるＩ／Ｏ（機器間入出力）インターフェースを対象としたものになる。

【００８２】ここで、「ｂａｃｋ－ｃｈａｎｎｅｌ２」の先に、キーボードとディスプレイとモデムを有するコンピュータ端末２１４を用意し、電話回線とＩＰＭＰＳ２０７とに接続する。この構成において、コンピュータ端末２１４は、認証の必要なストリーム中のオブジェク

トとその認証先の情報をＩＰＭＰＳ２０７から受け取り、その情報をディスプレイに表示する。操作者は、その表示を参照して、認証の必要なストリーム中のオブジェクトを選択する。コンピュータ端末２１４は、認証先に電話をかけて、認証方法やアクセスコードを該認証先から受け取り、その内容をディスプレイに表示する。操作者が、受け取った情報をキーボードを使って入力すると、その入力情報がＩＰＭＰＳ２０７に通知され、必要なオブジェクトに対するアクセスを許可状態にする。

【００８３】ここでは、電話回線を利用する場合を例として挙げたが、この代わりに、例えば、ＣＡＴＶのケーブルや無線通信路を利用しても良い。

【００８４】また、場合によっては、予め認証先との契約において入手したアクセス認証に必要な情報を格納したＰＣ　Ｃａｒｄをコンピュータ端末２１４内のＰＣＭＣＩＡインターフェースに差し込んで、アクセス認証に必要な情報をＩＰＭＰＳ２０７に通知して、オブジェクトに対するアクセスを許可状態にしてもよい。

【００８５】なお、操作時間や認証時間がある程度長くなる認証処理の場合は、ストリーム再生の開始時やシーンチェンジ時等、リアルタイムでない場合に有効である。

【００８６】このように、この実施の形態によれば、用途に応じて「ｂａｃｋ－ｃｈａｎｎｅｌ１」又は「ｂａｃｋ－ｃｈａｎｎｅｌ２」を選択して使用することができる。この選択は、操作者が行うことができるように構成してもよいし、システム内部で遅延時間限界等を考慮して最適な方を選択するようにしてもよい。

【００８７】以上のように、２種類の異なる「ｂａｃｋ－ｃｈａｎｎｅｌ」を設けることにより、柔軟性の高い認証処理を実現することができる。

【００８８】（第２の実施形態）以上説明したように、第１の実施形態においては、当該ＭＰＥＧ－４プレーヤーが、ネットワーク上の接続された１又は複数のサーバのうち対応するＵＲＬを持つサーバに対して認証依頼信号を送信する際に、「ｂａｃｋ－ｃｈａｎｎｅｌ」を用いる手法について説明したが、本第２の実施形態においては、「ｂａｃｋ－ｃｈａｎｎｅｌ」の他の利用方法について説明することにする。

【００８９】図８は、図２、３に対して、著作権保護システム（ＩＰＭＰ　Ｓｙｓｔｅｍ８６）とオブジェクトデータ処理フロー制御部（ＩＰＭＰ　Ｓｔｒｅａｍ　Ｆｌｏｗ　Ｃｏｎｔｒｏｌ８３）とを加えたＭＰＥＧ－４プレーヤーの概略図を示している。

【００９０】図８は、図４における「アクセスコントロールポイント」におけるストリームの制御の内容を、より具体的に開示したものである。この図８において、著作権保護を要求する画像オブジェクト符号化データを含むＭＰＥＧ－４ビットストリームはＤｅｍｕｘ　Ｌａｙｅｒ８１で各々のオブジェクトデータに分割され、Ｓｙｎｃ　Ｌａｙｅｒ８２で符号化やビットストリーム作成時に加えられた時間刻印情報に従ってプレーヤー内部時間に変換・同期される。

【００９１】一方、ＩＰＭＰ　Ｓｙｓｔｅｍ８６は、Ｄｅｍｕｘ　Ｌａｙｅｒ８１で分離された著作権保護情報に基づき、個々に分離された著作権保護を要求するオブジェクトデータの認証処理を行い、ＩＰＭＰ　Ｓｔｅａｍ　Ｆｌｏｗ　Ｃｏｎｔｒｏｌ８３へ許可信号を渡してオブジェクトデータ処理フロー制御を行い、Ｃｏｍｐｒｅｓｓｉｏｎ　Ｌａｙｅｒ８４にて、各オブジェクトデータは各オブジェクトデータ毎のデコーダで復号され、Ｃｏｍｐｏｓｉｔｉｏｎ　Ｌａｙｅｒ８５にて、復号されたシーン記述にしたがってシーン合成を行い、表示する。

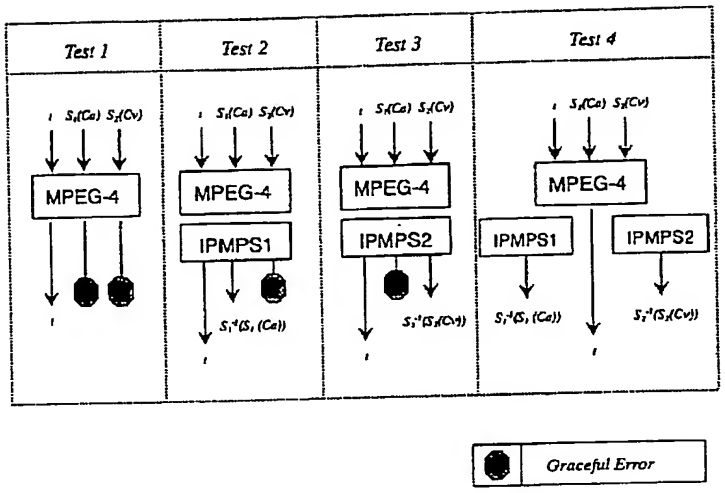
【００９２】特に、オブジェクトデータ処理フロー制御の方法には、幾つかの方法が考えられ、ここでは例として、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃１と＃２の２つを挙げて、解決しようとする問題の説明をする。

【００９３】表３は、ＩＰＭＰ　Ｓｙｓｔｅｍ（ＩＰＭＰＳ）とＳｔｒｅａｍ　ＦｌｏｗＣｏｎｔｒｏｌの関係を示す例として、４つのテストプランを示した図である。

【００９４】

【表３】

IPMP　Test　Plan



【００９５】この表３において、テスト１は、ＩＰＭＰ　Ｓｙｓｔｅｍが存在しない場合、テスト２は、ＩＰＭＰＳ１だけが存在する場合、テスト３は、ＩＰＭＰＳ２だけが存在する場合、テスト４は、ＩＰＭＰＳ１とＩＰＭＰＳ２の両方が存在する場合を示している。

【００９６】次に、各テストにおいて入出力する信号、及び、ＩＰＭＰＳ１とＩＰＭＰＳ２の役割の違いについて説明する。まず、表３では、Ｕｎｐｒｏｔｅｃｔｅｄ　Ｔｅｘｔ　Ｏｂｊｅｃｔ　Ｓｔｒｅａｍを”ｔ”と表現し、Ｐｒｏｔｅｃｔｅｄ　Ａｕｄｉｏ　Ｓｔｒｅａｍを”Ｓ１（Ｃａ）”と表現し、Ｐｒｏｔｅｃｔｅｄ　Ｖｉｄｅｏ　Ｓｔｒｅａｍを”Ｓ２（Ｃｖ）”と表現している。そして、Ｓ１（Ｃａ）用ＩＰＭＰ　Ｓｙｓｔｅｍを”ＩＰＭＰＳ１”と表現し、オリジナルの符号化データとＡＳＣＩＩ　ｃｏｄｅ　”ｘ”とのＸＯＲ（論理的排他和）の結果を”Ｓ１（Ｃａ）としている。従って解読キーはＡＳＣＩＩｃｏｄｅ　”ｘ”で、出力は、オリジナルの符号化データと”ｘ”との”ＸＯＲ”となる。

【００９７】また、Ｓ２（Ｃｖ）用ＩＰＭＰ　Ｓｙｓｔｅｍを”ＩＰＭＰＳ２”と表現し、オリジナルの符号化データとＡＳＣＩＩ　ｃｏｄｅ　”ａ”とのＸＯＲの結果を”Ｓ２（Ｃｖ）としている。従って解読キーはＡＳＣＩＩ　ｃｏｄｅ　”ａ”で、出力は、オリジナルの符号化データと”ａ”との”ＸＯＲ”となる。なお、”Ｇｒａｃｅｆｕｌ　Ｅｒｒｏｒ”とは、ｐｒｏｔｅｃｔｅｄ　ｏｂｊｅｃｔ　ｓｔｒｅａｍを正常にキーで解読できなかったために起こるデコーダ以降でのエラーで、いわゆる”ｆａｔａｌ　ｅｒｒｏｒ（致命的システムエラー）”ではなく、例えば、　Ｐｒｏｔｅｃｔｅｄ　Ｖｉｄｅｏ　Ｓｔｒｅａｍの場合の考えられる”Ｇｒａｃｅｆｕｌ　Ｅｒｒｏｒ”は、「表示されない」、若しくは、「乱れた画面が表示される」等のエラーである。テスト４の場合のみ、”Ｇｒａｃｅｆｕｌ　Ｅｒｒｏｒ”が発生しない。

【００９８】表４は、ＩＰＭＰのＶｅｒｉｆｉｃａｔｉｏｎテストのコンディションとパラメータを示した図である。

【００９９】

【表４】

IPMP Verification Test Condition and Parameters

Condition		Test 1	Test 2	Test 3	Test 4
Contents	Ct	Unprotected Text	<---	<---	<---
	S1(Ca)	Protected Audio	<---	<---	<---
	S2(Cv)	Protected Video	<---	<---	<---
IPMP Condition	IPMP-ES and IPMP-D	yes	yes	yes	yes
	IP Identification Data Set	yes	yes	yes	yes
	IPMP-S 1	none	XOR 'x' for S1(Ca)	none	XOR 'x' for S1(Ca)
	IPMP-S 2	none	none	XOR 'a' for S2(Cv)	XOR 'a' for S2(Cv)
Test Condition	#1	none	Embedded 'key' & constant delay	<---	<---
	#2	none	User interaction & non-fixed delay	<---	<---
	Synchronization	yes	yes	yes	yes
Expected result		Ct; pass S1(Ca); error S2(Cv); error	Ct; pass S1(Ca); pass S2(Cv); error	Ct; pass S1(Ca); error S2(Cv); pass	Ct; passs S1(Ca); pass S2(Cv); pass

【０１００】この表４において、テスト２を実行する場合、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ＃１では、各オブジェクトストリームにとって正常なキーが、あらかじめＩＰＭＰ　Ｓｙｓｔｅｍ（ＩＰＭＰＳ１，　ＩＰＭＰＳ２）に在り、入ってきたオブジェクトストリームを直ちに（また、一定の遅延時間で）「解読」して各デコーダに出力する。

【０１０１】また、テスト２を実行する場合、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃２では、各オブジェクトストリームにとって正常なキーが、あらかじめＩＰＭＰ　Ｓｙｓｔｅｍ（ＩＰＭＰＳ１，　ＩＰＭＰＳ２）にはなく、外部からのキー入力やスマートカード挿入等のユーザーインタラクティブな方法によって正常なキーを入力し、入ってきたオブジェクトストリームを「解読」して各デコーダに出力する。そのため、遅延時間は一定ではない。

【０１０２】図９は、ＭＰＥＧ－４　Ｓｙｓｔｅｍ　Ｐｌａｙｅｒの一例の内部機能ブロックダイヤグラムとデータの流れを示した図である。この図９は、同期メカニズムの説明のために、実際のシステムを簡略化して示したものであり、ＩＰＭＰ　Ｓｙｓｔｅｍとオブジェクトデータ処理フロー制御は省略してある。

【０１０３】まず、アプリケーションから起動されるＭＰＥＧ－４　Ｓｙｓｔｅｍ　Ｐｌａｙｅｒの入り口関数、Ｅｘｅｃｕｔｅ（）は、各機能モジュールを呼び起こし、データ領域バッファ確保や各機能関数へのメモリ割付などを行い、データ処理の準備をする。ＤＭＩＦｌａｙｅｒのＳｅｒｖｉｃｅ　ｍｏｄｕｌｅ関数としてのＦｌｅｘＤｅｍｕｘ９１によって、入力されるＭＰＥＧ－４ビットストリーム、即ち、ネットワークからのパケットデータやデータファイルは、一連のデータ群として受け取られ、ＡＬＭａｎａｇｅｒ９２へと渡される。

【０１０４】次に、ＡＬＭａｎａｇｅｒ９２内部で、データ群から各オブジェクトデータ、例えば、ビデオデータ、オーディオデータ、シーン記述データ等のデータの分割され、各データチャネルとなってシーン記述やオブジェクト関連情報データは、ＢＩＦＳＤｅｃｏｄｅｒ９３へ、ビデオ、オーディオデータはＤｅｃｏｄｅｒ９４へ渡される。

【０１０５】ＢＩＦＳＤｅｃｏｄｅｒ９３及びＤｅｃｏｄｅｒ９４で復号されたシーン記述情報と、ビットストリーム作成時に加えられた時間刻印情報に応じて、Ｐｒｅｓｅｎｔｅｒ９５やＭｅｄｉａ　Ｓｔｒｅａｍデータ処理部（不図示）で、各復号Ｍｅｄｉａ　Ｏｂｊｅｃｔ　ｄａｔａ（Ｖｉｄｅｏ，　Ａｕｄｉｏ　ｄａｔａ）の時間関係を調整し、同期を取り、シーン合成する。

【０１０６】図１０は、上記一連のデータ処理プロセスを簡略化したものである。この図１０において、ＦｌｅｘＤｅｍｕｘ９１は、ＭＰＥＧ－４ビットストリームを受け取り、各オブジェクトデータ毎のｅｌｅｍｅｎｔａｒｙ　ｓｔｒｅａｍ（ＥＳ）に分ける。そして、ＡＬＭＡｎａｇｅｒ９２は、各オブジェクトデータ毎のＥＳをデコード単位に分割し、ＢＩＦＳＤｅｃｏｄｅｒ９３及びＤｅｃｏｄｅｒ９４は、各オブジェクト毎の復号処理を行う。そして、各オブジェクトデータ毎の復号されたデータ群Ｍｅｄｉａ　Ｓｔｒｅａｍが生成され、Ｐｒｅｓｅｎｔｅｒ９５は、　Ｍｅｄｉａ　Ｓｔｒｅａｍデータを扱う”ＭｅｄｉａＳｔｒｅａｍＩｍｐ：：Ｆｅｔｃｈ（）”関数を用いて、個々のオブジェクトデータの時間調整を行い、各オブジェクトデータを１シーン毎に合成し、表示する。

【０１０７】図１１は、時間調整のデータ処理例を示す図である。この図１１を用いて、Ｐｒｅｓｅｎｔｅｒ９５における時間調整処理について詳しく説明する。まず、ステップＳ１１０１において、Ｓｙｓｔｅｍ　Ｐｌａｙｅｒの現在時間に許容値を加え（→ｄｗＣｕｒｒｅｎｔＴｉｍｅ）、その値に基づいて、ステップＳ１１０２において、処理予定データ（ＡＵ）の刻印時間（Ｔｉ

ｍｅＳｔａｍｐ）をＳｙｓｔｅｍ　Ｐｌａｙｅｒ時間に換算し（→ｄｗＴｉｍｅ）、　ステップＳ１１０４において、現在時間（ｄｗＣｕｒｒｅｎｔＴｉｍｅ）と処理予定データ（ＡＵ）の刻印時間（ｄｗＴｉｍｅ）とを比較する。処理予定データ（ＡＵ）の刻印時間（ｄｗＴｉｍｅ）が現在時間（ｄｗＣｕｒｒｅｎｔＴｉｍｅ）より後であれば、ステップＳ１１０６に進み、実際のシーン合成処理を行い、処理予定データ（ＡＵ）の刻印時間（ｄｗＴｉｍｅ）が現在時間（ｄｗＣｕｒｒｅｎｔＴｉｍｅ）より前であれば、シーン合成に不適（時間的にシーン合成時間に間に合わないデータと判断）として、ステップＳ１１０５に進み、次のデータ処理ブロック（ＡＵ）を処理対象にする。

【０１０８】図１２は、図１１に示した時間調整処理について、タイムチャートで時系列に示したものである。この図１２において、Ｏｂｊｅｃｔ　ｓｔｒｅａｍ（ＡＵ０）は、Ａｒｒｉｖａｌ（ＡＵ０）の時点で、ＢＩＦＳＤｅｃｏｄｅｒ９３若しくはＤｅｃｏｄｅｒ９４のＤｅｃｏｄｉｎｇ　Ｂｕｆｆｅｒ１２０１へ届き、その後デコードされて、エンコード時に付加された刻印時間ＤＴＳ（ＡＵ０）の時点で、Ｐｒｅｓｅｎｔｅｒ９５のＣｏｍｐｏｓｉｔｉｏｎ　Ｍｅｍｏｒｙ１２０２へ送られ、シーン合成時間ＣＴＳ（ＣＵ０）の時点から、シーン合成される。そして、続くＯｂｊｅｃｔ　ｓｔｒｅａｍ（ＡＵ１）も同様に、ＤＴＳ（ＡＵ１）の時点でＤｅｃｏｄｉｎｇ　Ｂｕｆｆｅｒ１２０１からＣｏｍｐｏｓｉｔｉｏｎ　Ｍｅｍｏｒｙ１２０２へと移され、ＣＴＳ（ＣＵ１）からシーン合成される。

【０１０９】このように、図１２を見れば、図１１において、Ｄｅｃｏｄｉｎｇ　Ｂｕｆｆｅｒ１２０１における時間ＤＴＳが、実際の現在時点ｄｗＣｕｒｒｅｎｔＴｉｍｅ以降として、Ｃｏｍｐｏｔｓｉｔｉｏｎ　Ｍｅｍｏｒｙ１２０２における実際のシーン合成時間ＣＴＳへと調整されていることが分かる。

【０１１０】図１３は、図１０に示した処理フローにＩＰＭＰ　Ｓｙｓｔｅｍでの処理を加えたものである。具体的には、以下のような処理を行う。ＦｌｅｘＤｅｍｕｘ９１がＭＰＥＧ－４ビットストリームを受け取り、各オブジェクトデータ毎のＥｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ（ＥＳ）に分け、ＡＬＭａｎａｇｅｒ９２が各オブジェクトデータ毎のＥＳをデコード単位に分割するところまでは、図１０と同様である。そして、次に、ＡＬＭａｎａｇｅｒ９２で分けられたオブジェクトデータから、特にＩＰＭＰ関連情報に基づいて、ｐｒｏｔｅｃｔｅｄ　ｓｔｒｅａｍを特定し、正常キーの入力・認証等のＩＰＭＰ　Ｓｙｓｔｅｍ処理を行う。そして、ＢＩＦＳＤｅｃｏｄｅｒ９３及びＤｅｃｏｄｅｒ９４が、各オブジェクトデータ毎のデコードするデータ群であるＭｅｄｉａＳｔｒｅａｍを復号処理して、Ｐｒｅｓｅｎｔｅｒ９５が、個々のオブジェクトの時間調整を行い、１シーン毎に合成し表示する。

【０１１１】ここで、一例として、表４に示したテスト２を実行した場合におけるＴｅｓｔＣｏｎｄｉｔｉｏｎ　＃１と＃２のオブジェクトデータ処理フロー制御について説明する。まず、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ＃１の方法では、キー解読の時間は各ＩＰＭＰ　Ｓｙｓｔｅｍ毎に一定の遅延としてデコーダへ伝えられるので、図８のＣｏｍｐｏｓｉｔｉｏｎ　Ｌａｙｅｒ８４や、図９のＰｒｅｓｅｎｔｅｒ９５で吸収される範囲であるように全体の遅延を見込んでおけば、結果として同期の問題は起こらない。

【０１１２】一方、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ＃２の方法では、以下のようになる。図１４は、テスト２をＴｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃２で実行する場合のＩＰＭＰ　Ｓｙｓｔｅｍの処理を説明したフローチャートである。まず、ステップＳ１４０１において、ＡＬＭａｎａｇｅｒ９２でデコード単位に分割された各オブジェクト毎のストリームを得る。そして、ステップＳ１４０２において、正当なキー入力があったか否かを判別する。そして、正当なキー入力ではなかった場合は、ステップＳ１４０３に進み、ｐｒｏｔｅｃｔｅｄ　ｓｔｒｅａｍの解読をしないで、ＨＯＬＤする。また、正当なキー入力があった場合は、ステップＳ１４０４に進み、ｐｒｏｔｅｃｔｅｄ　ｓｔｒｅａｍの解読を行い、次の処理へと進む。

【０１１３】テスト２をＴｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃２で実行する場合に、図１４に示したフロー制御が行われる場合には、正常なキー入力があるまでのストリームはｓｕｓｐｅｎｄされ、一方、ｎｏｎ－ｐｒｏｔｅｃｔｅｄ　ｓｔｒｅａｍや他の既に正常なキー入力によって認証・解読されたストリームは次のデコーダ処理、シーン合成のための時間同期処理へと移行する。この際、先のｓｕｓｐｅｎｄｅｄ　ｓｔｒｅａｍが正常なキー入力で認証・解読され、次の処理へ移行するまでの経過時間は、各ｐｒｏｔｅｃｔｅｄ　ｓｔｒｅａｍへのユーザーインタラクティブな操作のために、各々一定ではなく、また処理再開時点では、すでにｄｗＴｉｍｅがｄｗＣｕｒｒｅｎｔＴｉｍｅを過ぎていることも考えられる。

【０１１４】この場合、図１１及び図１２から明らかなように、再開されたストリームは少なくとも再開以降のｄｗＴｉｍｅがｄｗＣｕｒｒｅｎｔＴｉｍｅより後となるまでデコードされず、次の処理予定データ（ＡＵ）までスキップし（即ち、データが間引かれ）、スキップされた部分については、シーン合成されることはない。このように、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ＃２の方法では、一部のデータが間引かれてしまい、連続するコンテンツを最初から得ることができなくなる。

【０１１５】もちろん、有料放送のような”ｐｕｓｈ”型のデータ配信では、基本的に時間帯に応じた片方向デ

一タ配信で、セットトップボックス等の認証機能付き受像システムでデータを受けるので、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃１で十分対応できるため問題はない。

【０１１６】しかしながら、例えば、視聴者が、インターネット上ホームページの、ある映画などの映像の初めの数分間のコマーシャルデモコンテンツ群を見て、その中から１つのコンテンツを選択して、課金認証後に、その映像を初めから入手・鑑賞したいような場合は、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃１では無論対応できないし、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃２では選択・認証後に再生を再開するため、視聴者は、それ迄に流れてしまったコンテンツを得ることができない。

【０１１７】また、ＭＰＥＧ－４では、ビデオオブジェクト毎の選択・再生が可能なので、先のコマーシャルデモコンテンツにおいては、認証処理されていない状態でも、人物や背景など、一部のオブジェクトだけをｐｒｏｔｅｃｔｅｄ　ｓｔｒｅａｍとしてｇｒａｃｅｆｕｌ　ｅｒｒｏｒとして再生させ続けることが可能であるが、この場合でも、Ｔｅｓｔ　Ｃｏｎｄｉｔｉｏｎ　＃２では、選択・認証後に再生を再開するため、視聴者は、それ迄に流れてしまった正常かつ完全なフルコンテンツを得ることができない。このように、視聴者が、最初から完全なコンテンツを見たいと思った場合には、コンテンツ配信側のサーバに、最初から映像を再送するように指示する必要がある。

【０１１８】一般的な解決方法の一つは、選択・認証後の映像再生の再開時に、クライアント（ユーザ）側からサーバ（コンテンツ配信）側へとフルコンテンツの再送要求をすることであるが、通常、この要求を行うためには、サーバ側がクライアント側からの要求を受け取るために、サーバ側がクライアント側へ予めアプリケーションを提供しておく必要がある。

【０１１９】しかしながら、ＭＰＥＧ－４などのように複数のビデオオブジェクトコンテンツやオーディオオブジェクトコンテンツを各々異なるＵＲＬ（ＵｎｉｆｏｒｍＲｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）先から得てシーン合成する場合では、複数のコンテンツ配信のサーバの夫々に対するアプリケーションと認証・再送方法が必要となるので、プログラム管理が煩雑となり、方法としては現実的ではない。

【０１２０】そこで、本第２の実施形態では、そのような、最初から映像を再送するように指示する信号を、その要求先のサーバのＵＲＬの情報と、認証結果を示す情報とともに、第１の実施形態で説明した「ｂａｃｋ－ｃｈａｎｎｅｌ」（「ｂａｃｋ－ｃｈａｎｎｅｌ１」または「ｂａｃｋ－ｃｈａｎｎｅｌ２」）を使用して、コンテンツ配信元のサーバへと送信するのである。

【０１２１】より具体的には、本第２の実施形態においては、通常の使用ではＭＰＥＧ－４ビットストリームを受け取ってシーン再生処理する（ｄｏｗｎｓｔｒｅａｍ処理する）プレーヤー側から、ＭＰＥＧ－４でのｂａｃｋ　ｃｈａｎｎｅｌ機能を使って、プレーヤー側からサーバ側へと情報を配信する（即ち、図１に示したようなＵｐｃｈａｎｎｅｌ　ｉｎｆｏｒｍａｔｉｏｎで、認証・再送情報をＵｐｓｔｒｅａｍ処理する）ことで、各コンテンツ配信元サーバ側では、認証・再送情報の通信に関する部分を、ＩＰＭＰ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅと共に共有することとなり、プログラム管理の煩雑さを軽減することができる。

【０１２２】このように、第２の実施形態によれば、認証処理後に、ネットワークを介して著作物の再送要求を行うことが容易にできるので、認証処理に関わる遅延時間によって、再生される映像が欠落するといったことがなくなる。

【０１２３】なお、第２の実施形態においては、認証処理の方法については、特に問わない。即ち、第１の実施形態のように、ネットワークを介して各コンテンツ配信サーバに対して認証依頼信号を送って、該各コンテンツ配信サーバからアクセス許可をもらうのでもよいし、また、ＭＰＥＧ－４プレーヤーの方に、予め正当なキーが記憶されていて、視聴者がローカルに認証作業を行うようにするのでも構わない。

【０１２４】なお、本発明は、複数の機器から構成されるシステムに適用しても、一つの機器からなる装置に適用してもよい。

【０１２５】また、上記の実施の形態に係る装置又は方法を構成する構成要素の全体のうち一部の構成要素で構成される装置又は方法も、本件出願に係る発明者が意図した発明である。

【０１２６】また、上記の実施の形態に係る装置の機能は、プログラムコードを記録した記憶媒体をシステム或いは装置に固定的又は一時的に組み込み、そのシステム或いは装置のコンピュータ（又はＣＰＵ若しくはＭＰＵ）が該記憶媒体に格納されたプログラムコードを読み出して実行することによっても達成される。ここで、該記憶媒体から読み出されたプログラムコード自体或いは該記憶媒体自体が法上の発明を構成する。

【０１２７】プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等が好適であるが、他のデバイスを採用することもできる。

【０１２８】また、コンピュータが記憶媒体から読み出したプログラムコードを実行することにより本発明の特有の機能が実現される場合のみならず、そのプログラムコードによる指示に基づいて、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部又は全部を負担する実施の態様も本発明の技術的範囲に属する。

【０１２９】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備えられたメモリに書込まれた後に、そのプログラムコードの指示に基づいて、その機能拡張ボードや機能拡張ユニットに備えられたＣＰＵ等が実際の処理の一部又は全部を負担する実施の態様も本発明の技術的範囲に属する。

【０１３０】

【発明の効果】以上説明したように、本発明によれば、認証処理を効率化し、著作権等を有効に保護すると共に著作物等を有効に利用することができる。さらに本発明によれば、認証処理後に、ネットワークを介して著作物の再送要求を行うようにしたことにより、認証処理に関わる遅延時間による再生映像の欠落がなくなり、そのことにより、多くの認証処理方法が可能となる効果がある。

【０１３１】

【図面の簡単な説明】

【図１】従来のデジタル映像データの送受信システムを示す図である。

【図２】従来のＭＰＥＧ－４プレーヤーの構成図である。

【図３】図２を模式化・簡略化した図である。

【図４】本発明の好適な実施の形態に係るback channelを行うＭＰＥＧ－４プレーヤーの構成図である。

【図５】リモートアクセスを説明するための簡略図である。

【図６】ＵＲＬ先で更にＵＲＬ指定がある場合の階層構造の例を示す図である。

【図７】認証処理に関するクライアントの動作を示すフローチャートである。

【図８】図３の構成にIPMP System処理部を追加した構成を示す図である。

【図９】MPEG-4 プレーヤーの内部機能ブロックダイヤグラムとデータの流れを示す図である。

【図１０】図５におけるデータ処理プロセスを簡略化して示した図である。

【図１１】MPEG-4オブジェクトアクセスデータユニットの時間調整動作例を示すフローチャートである。

【図１２】Decoding BufferとComposition Memroyのデータ移動とタイミングを示す図である。

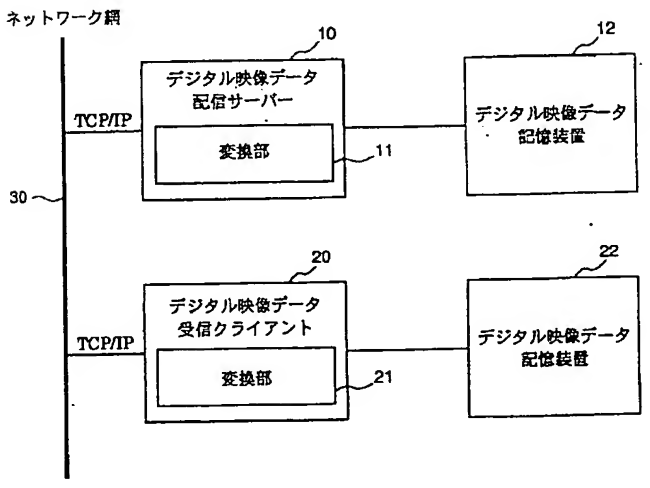
【図１３】図６にIPMP System処理部を加えた場合のデータ処理プロセスを示す図である。

【図１４】図８のIPMP Systemの動作例をしめすフローチャートである。

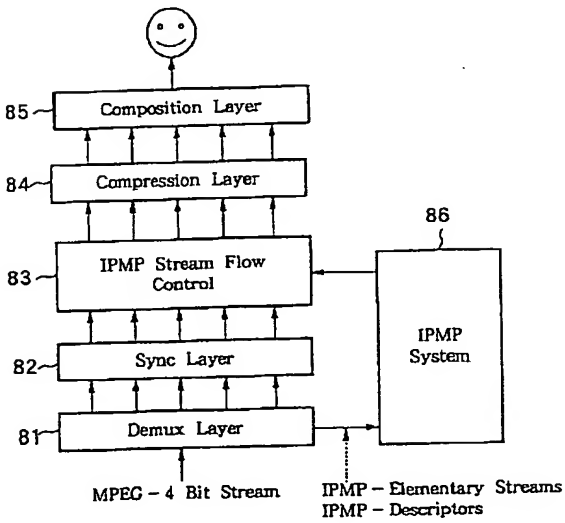
【符号の説明】

１０　デジタル映像データ配信サーバー
１１、２１　変換部
１２、２２　デジタル映像データ記憶装置１２
２０　デジタル映像データ受信クライアント
３０　ネットワーク網
２０１　マルチプレクサ
２０２～２０４　ネットワーク・サイト
２０６　デマルチプレクサ
２０８　シーン・ディスクリプタ
２０９　オーディオ・ビジュアル・デコーダ
２１０　オブジェクトディスクリプタ

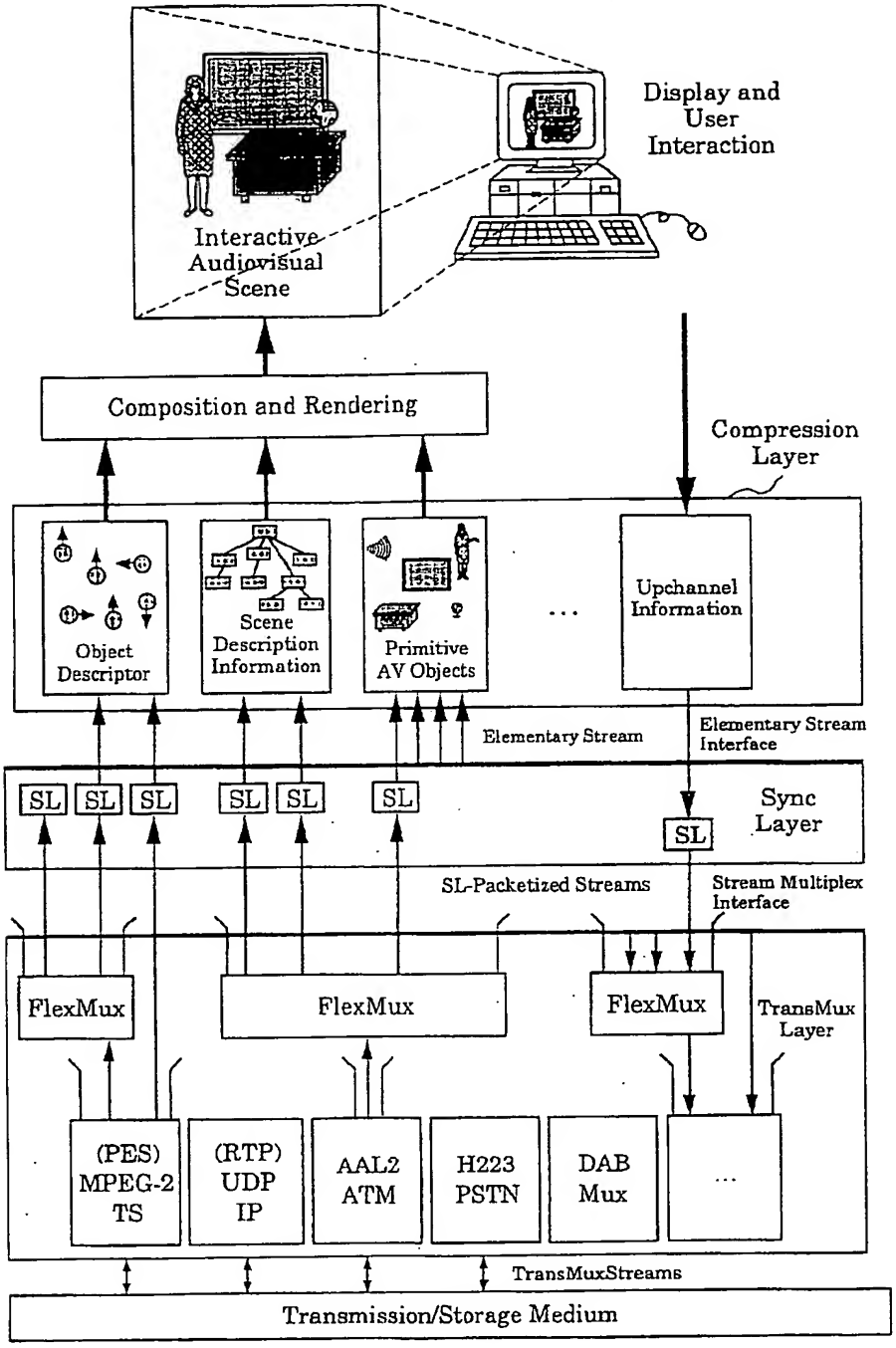
【図１】



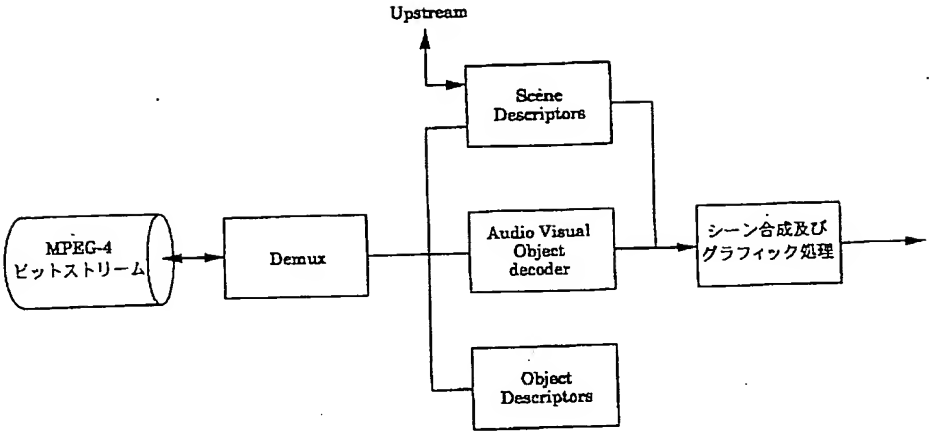
【図８】



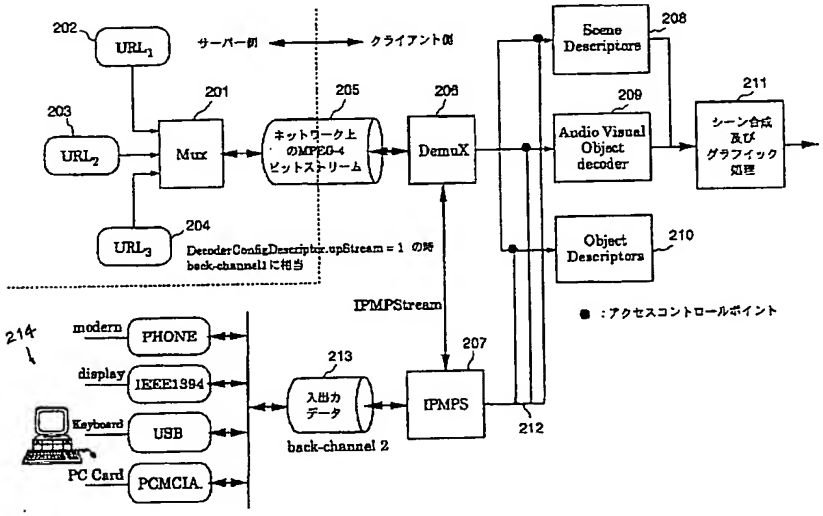
【図２】


Display and User Interaction
Interactive Audiovisual Scene
Composition and Rendering
Compression Layer
Object Descriptor
Scene Description Information
Primitive AV Objects
...
Upchannel Information
Elementary Stream
Elementary Stream Interface
SL
Sync Layer
SL-Packetized Streams
Stream Multiplex Interface
FlexMux
FlexMux
FlexMux
TransMux Layer
(PES) MPEG-2 TS
(RTP) UDP IP
AAL2 ATM
H223 PSTN
DAB Mux
...
TransMuxStreams
Transmission/Storage Medium

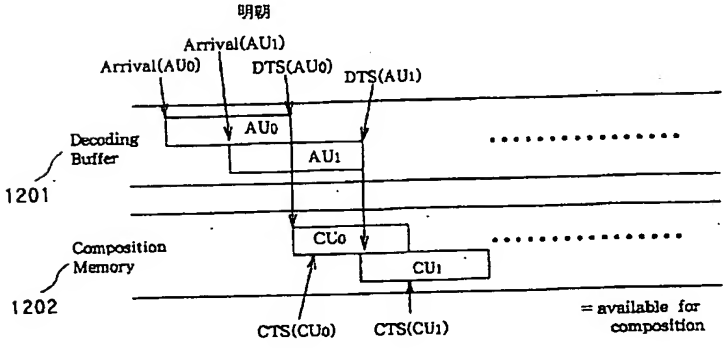
【図３】


Upstream
Scene Descriptors
MPEG-4 ビットストリーム
Demux
Audio Visual Object decoder
シーン合成及び グラフィック処理
Object Descriptors

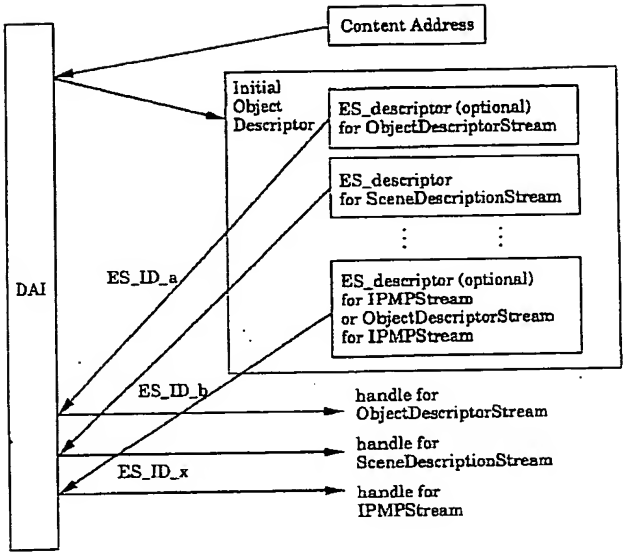
【図４】


202
URL1
サーバー側
クライアント側
201
205
206
203
URL2
Mux
ネットワーク上のMPEG-4 ビットストリーム
DemuX
204
URL3
DecoderConfigDescriptor.upStream = 1 の時 back-channel1に相当
Scene Descriptors
208
209
Audio Visual Object decoder
211
シーン合成及び グラフィック処理
Object Descriptors
210
IPMPStream
● :アクセスコントロールポイント
214
modern
PHONE
display
IEEE1394
Keyboard
USB
PC Card
PCMCIA
213
入出力データ
back-channel 2
207
IPMPS
212

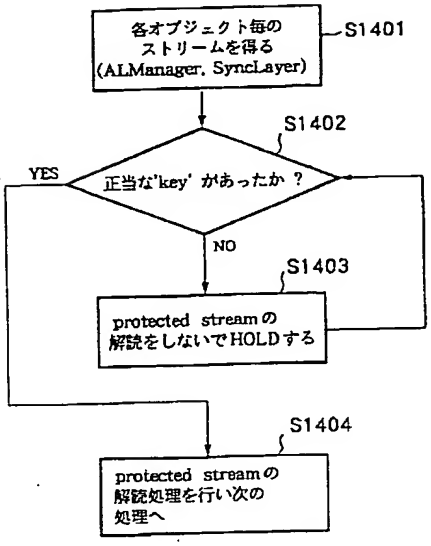
【図１２】


明朝
Arrival(AU1)
Arrival(AU0)
DTS(AU0)
DTS(AU1)
AU0
AU1
Decoding Buffer
1201
CU0
CU1
Composition Memory
1202
CTS(CU0)
CTS(CU1)
= available for composition

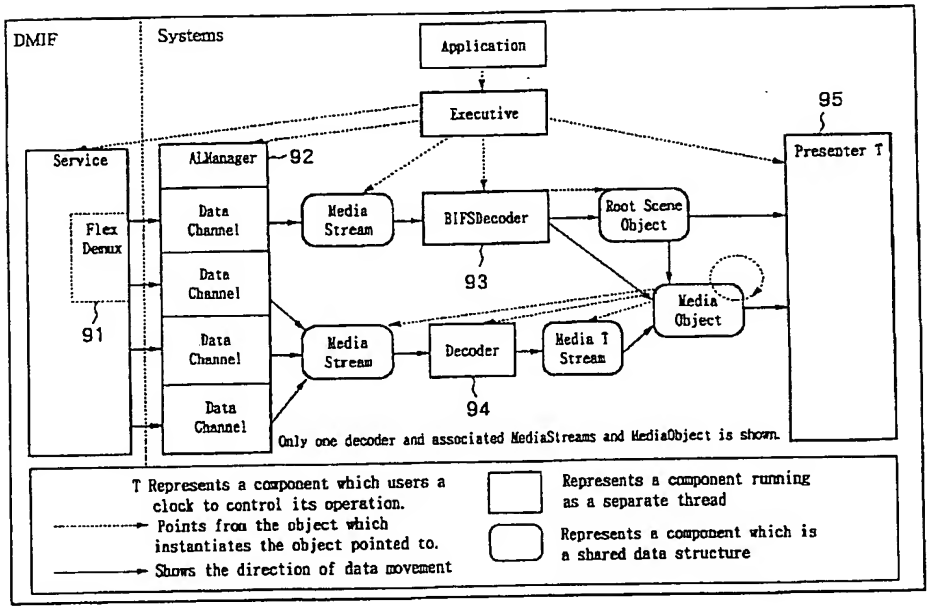
【図５】


Content Address
Initial Object Descriptor
ES_descriptor (optional) for ObjectDescriptorStream
ES_descriptor for SceneDescriptionStream
ES_descriptor (optional) for IPMPStream or ObjectDescriptorStream for IPMPStream
DAI
ES_ID_a
ES_ID_b
ES_ID_x
handle for ObjectDescriptorStream
handle for SceneDescriptionStream
handle for IPMPStream

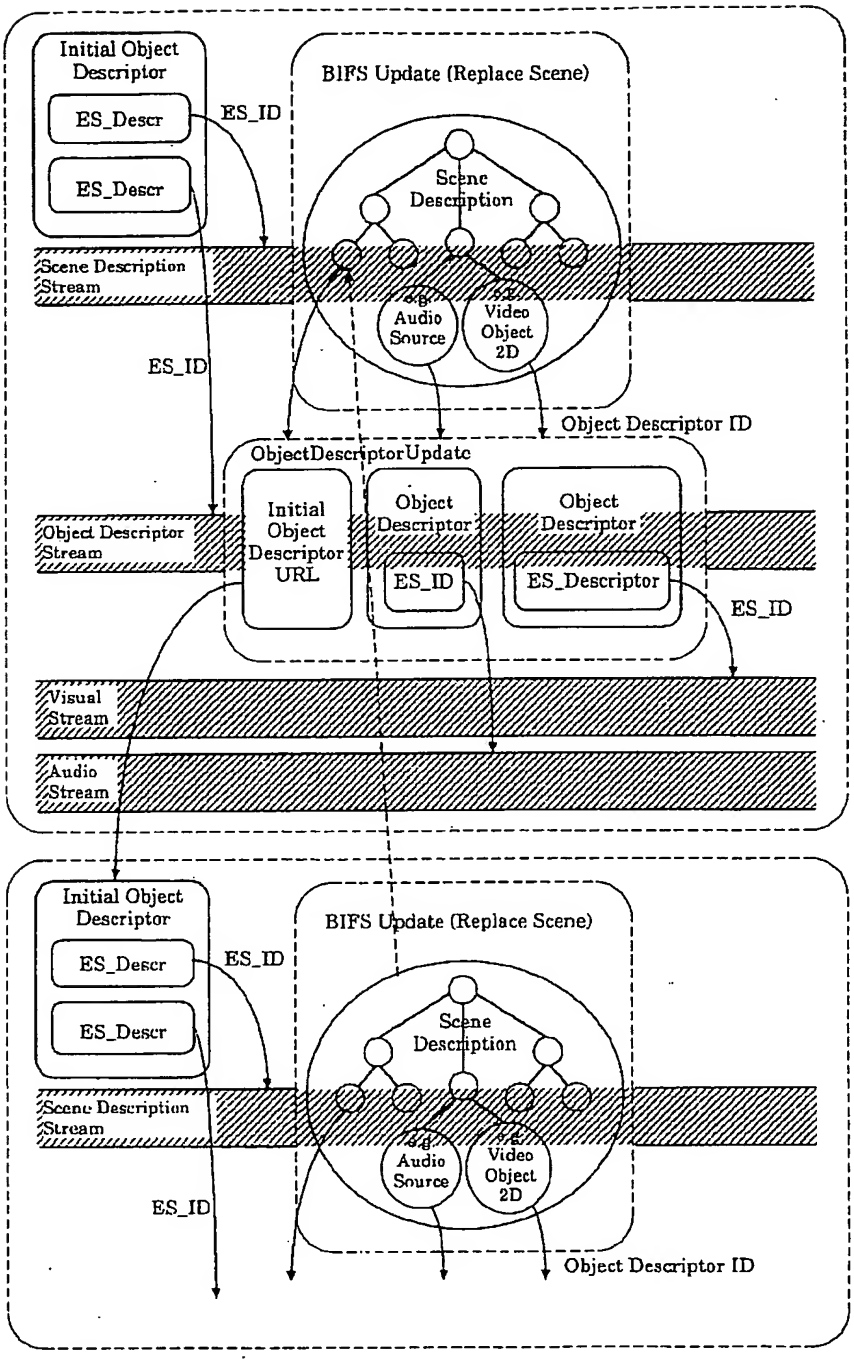
【図１４】


各オブジェクト毎のストリームを得る (ALManager, SyncLayer)
S1401
S1402
正当な'key'があったか？
YES
NO
S1403
protected streamの解読をしないでHOLDする
S1404
protected streamの解読処理を行い次の処理へ

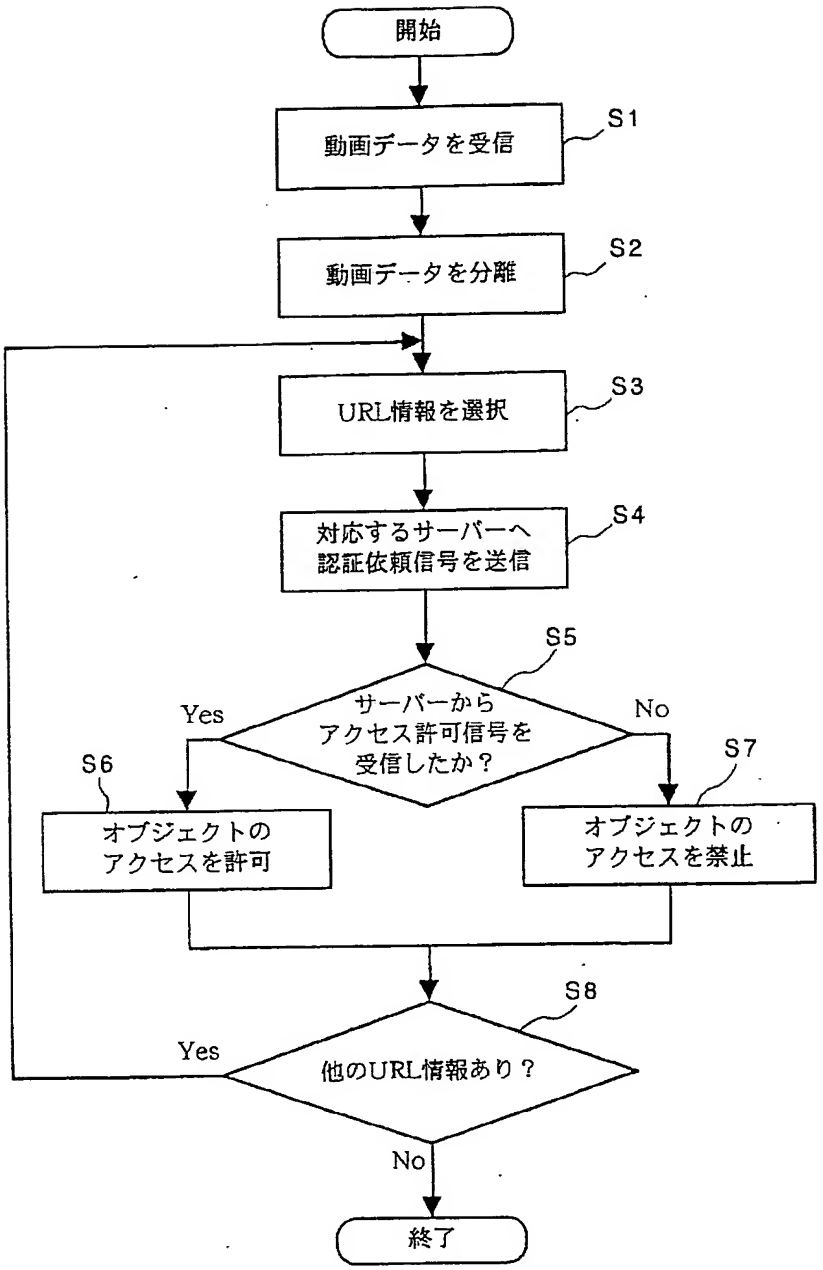
【図９】


DMIF
Systems
Application
Executive
95
Presenter T
Service
ALManager
92
Flex Demux
91
Data Channel
Data Channel
Data Channel
Data Channel
Media Stream
BIFSDecoder
Root Scene Object
93
Media Object
Media Stream
Decoder
Media T Stream
94
Only one decoder and associated MediaStreams and MediaObject is shown.
T Represents a component which users a clock to control its operation.
Points from the object which instantiates the object pointed to.
Shows the direction of data movement
Represents a component running as a separate thread
Represents a component which is a shared data structure

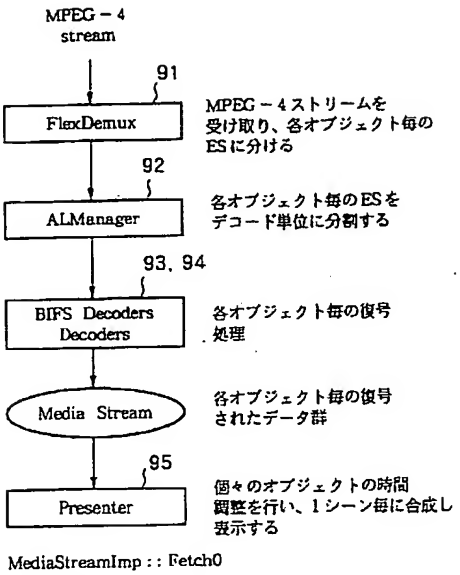
【図６】


Initial Object Descriptor
ES_Descr
ES_Descr
ES_ID
BIFS Update (Replace Scene)
Scene Description
Scene Description Stream
Audio Source
Video Object 2D
ES_ID
Object Descriptor ID
ObjectDescriptorUpdate
Initial Object Descriptor URL
Object Descriptor
ES_ID
Object Descriptor
ES_Descriptor
ES_ID
Object Descriptor Stream
Visual Stream
Audio Stream
Initial Object Descriptor
ES_Descr
ES_Descr
ES_ID
BIFS Update (Replace Scene)
Scene Description
Scene Description Stream
Audio Source
Video Object 2D
ES_ID
Object Descriptor ID

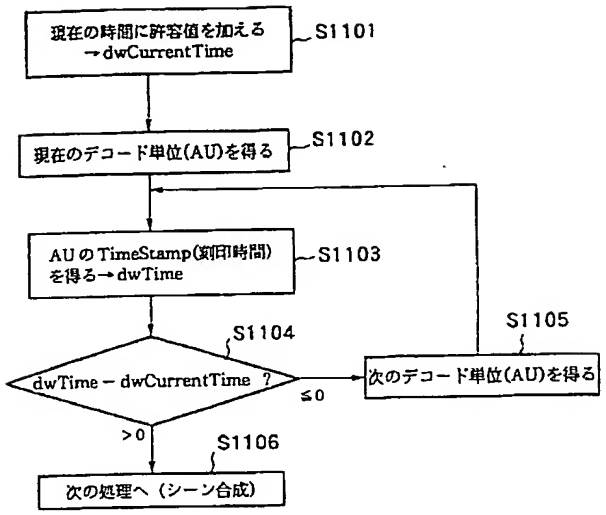
【図７】


開始
動画データを受信
S1
動画データを分離
S2
URL情報を選択
S3
対応するサーバーへ
認証依頼信号を送信
S4
S5
サーバーから
アクセス許可信号を
受信したか？
Yes
No
S6
S7
オブジェクトの
アクセスを許可
オブジェクトの
アクセスを禁止
S8
Yes
他のURL情報あり？
No
終了

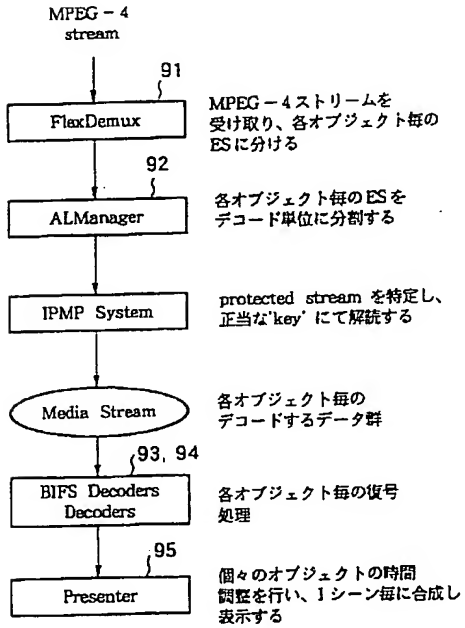
【図１０】



【図１１】



【図１３】



フロントページの続き

(51) Int. Cl.⁷		識別記号	F I		テーマコード（参考）
H04N	5/93		H04N	5/91	P
	7/24			5/93	E
	7/173	610		7/13	Z